ACEEE

Proc. of Int. Conf. on Advances in Computer Science, AETACS

An Overview of Visual Cryptography based Video Watermarking Schemes: Techniques and Performance Comparison

Adrita Barari 1, Sunita Dhavale 2
1 Dept. of Electronics Engineering, Defence Institute of Advanced Technology, Pune- 411025, India
Email: mailadrita@gmail.com
2 Dept. of Computer Engineering, Defence Institute of Advanced Technology, Pune- 411025, India
Email: sunitadhavale@diat.ac.in

***Abstract*— Digital communication has seen exponential growth in the past decade. Consequently, the security of digital data has become a field of extensive research since piracy and unauthorized use of such data is prevalent because of the ease with which data can be replicated or tampered. Visual Cryptography (VC) is a special cryptographic technique where decryption is done by an authorized user by simply overlaying the shares. Thus, there is no requirement for complex computations unlike normal cryptography. Though simple for an authorized user, it is equally difficult for an unauthorized user to attack since the secret message can be deciphered if and only if all the shares are available to the attacker. The probability of this is negligibly small since one of the shares usually needs to be registered with a Certified Authority (CA). The procedure is non- intrusive and does not alter the contents of the host image or video. For this reason, VC has been applied to image watermarking widely. In case of video watermarking applications, robustness against different types of attacks like frame attacks, spatial and temporal desynchronization attacks, statistical analysis and collusion attacks need to be considered. Also creation of shares for videos requires feature extraction techniques which are different from that of images. Moreover, as size of video is more, a large secret payload can be used to construct a share. In this survey paper, the research being carried out globally on VC techniques for videos, along with their pros and cons have been highlighted. The paper also discusses challenges in applying VC for video watermarking. Further, a performance comparison amongst the mentioned schemes is also provided.**

***Index Terms*— Visual Cryptography, Steganography, Video Watermarking, Peak Signal to Noise Ratio (PSNR), Normalised Correlation (NC), Mean Square error (MSE).**

I. INTRODUCTION

In today's world, a major part of communication is through digital data. Since replicating, tampering or changing such digital data does not require any expertise, it becomes absolutely necessary to have a preservation of Intellectual Rights for these. Instead of following Digital Rights Management (DRM) where content is merely encrypted, it is desirable to embed high security information into the digital content such that it is inseparable. This protection system is termed as watermarking [1]. Principles of watermarking help to realize unobtrusive communication systems which instead of performing just encryption, seek to keep the very existence of the message undisclosed. It has an additional advantage over encryption because watermarking is a means for content protection even after data has been decrypted. The role of watermarking

DOI: 02.AETACS.2013.4.113

complements (and does not replace) encryption. In fact, the historical roots of digital watermarking are derived mainly from, the science of information hiding or steganography and are of major consequence from a defence point of view.

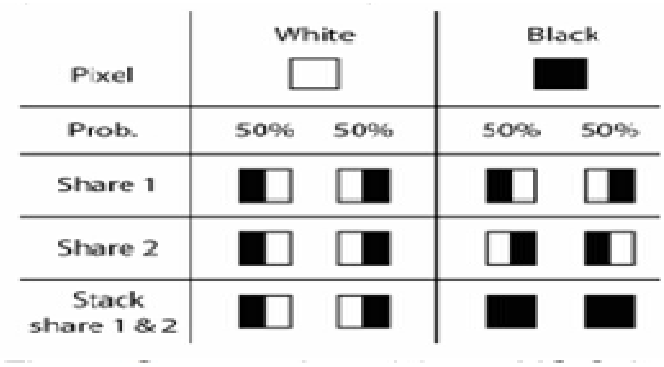

Figure 1.Construction of shares in a (2, 2) VC Scheme

Data payload, fidelity and robustness are the main parameters that must be considered in digital watermarking. Data payload refers to the number of bits of information that can be embedded via the watermark. Fidelity is the imperceptibility to human observation even after distortion of the watermark while robustness is the resilience of the watermark against attacks. Attacks on digital watermarks can be broadly classified into categories like removal attacks, geometric attacks, cryptographic attacks, protocol attacks and estimation based attacks. A watermark should be robust to all kinds of attacks and watermarking schemes should be so designed such that it should be impossible to remove the watermark without severe quality degradation of the cover content.

Naor and Shamir [2] proposed a lossless watermarking technique called visual cryptography (VC) in order to protect the security of a binary watermark secret image. The major advantage of this technique is that it does not modify the original image and decryption is done by human visual system. Here, a binary secret image is divided into two sets called shares as shown in Fig. 1. The shares have a pseudorandom noise like pattern and do not reveal any meaningful information alone. However, when all the shares are printed upon transparencies and overlaid one upon the other, they reveal the secret image.

Visual cryptography requires no previous knowledge or experience of cryptography on the part of the person decoding the message. Preparation of shares is a simple process which can be done with the help of the simple mathematical techniques proposed in [2]. At the decryption end, the job is performed not by complex cryptographic algorithms but by the human visual system, thus making the system both secure and simple. For Naor's *(k, n)* visual secret sharing approach, any *k* dealers can view the image by stacking them but anything less than *k* shares cannot reveal any information. Researchers later on, developed variants of the above mentioned scheme for image watermarking due to its sheer robustness, transparency, capacity to distinguish between different watermarks, simplicity and non-intrusiveness. This class of watermarks came to be known as *perceptual watermarks* since they used perceptual information based on human visual models for establishing copyright.

In this paper, section 2 discusses a brief literature review on VC based image watermarking techniques while section 3 presents detailed overview of existing VC based video watermarking schemes. A performance comparison amongst the mentioned VC based video watermarking schemes is provided in Section 4 followed by the conclusions drawn in Section 5.

II. Visual Cryptography Based Image Watermarking Schemes

Watermarking in images can be done both in spatial and transform domains. Spatial domain techniques though computationally less complex, are less resilient to attacks. Transform domain techniques, on the other hand, are more robust in comparison to spatial domain techniques since they modify the coefficients of the transform of the pixel values. Discrete wavelet transform (DWT), discrete cosine transform (DCT) and discrete Fourier transform (DFT) based transformed domain techniques have been found to be more robust than spatial domain techniques particularly in attacks like lossy compression, rescaling, rotation, noise addition etc.

To perform watermarking in images, researchers over the years have attempted to incorporate Naor and Shamir's [2] unique Visual Secret Sharing (VSS) technique in watermarking schemes to protect the security of their multimedia content. Many VC based watermarking schemes have been proposed for images in the literature [3-7]. In the *(k,n)* basic model [2], any *'k'* shares could decode the secret information. To improve the level of security, the basic model was extended to general access structures [3] where an access structure was a structure which deemed only certain shares as qualified. Retrieval of the secret was possible by stacking only the qualified shares. Modified VC based schemes were suggested by developers to partition the watermark into two pseudorandom noise-like shares. The first share was embedded in some specific pixels of the host image by decreasing their gray level values. The watermark was retrieved by superimposing the watermarked image and the second share. These methods had the drawback that it affected the host image data by embedding first share directly into the host image. Hence it was intrusive in nature. Later, a blind, non-intrusive VC based watermarking scheme was proposed where MSBs of selected pixels of host image were used to generate shares. To retrieve the watermark, the receiver needed both the secret key and the registered verification information simultaneously. Research was carried out in the following years to devise VC based copyright protection schemes where sampling distribution of means calculated from host image was used as a feature to form the shares. The scheme could register multiple secret images without altering the host image. In addition, this scheme had the advantage that the size of the watermark was not restricted by the size of the host image, i.e. binary image of any size can be used as a watermark.

In the conventional VSS schemes discussed above, the techniques revealed either the entire secret image or nothing, and hence limited level of secrecy which could be achieved. Fang and Lin [4] proposed a progressive visual secret sharing (PVSS) scheme which demonstrated that when more shares are stacked progressively, the recovery of the secret image would be clearer and clearer. Although Fang and Lin's method could achieve a progressive effect, their adoption of expanding pixels meant that more transmission time and storage space was needed. To overcome the disadvantages of [4], Hou and Quan [5] came up with a PVSS scheme with unexpanded shares which reduced storage space of shares, transmission time, bandwidth required for transmission and also was effective in maintaining the quality of the recovered image. In this method, it was noted that when any k ($k = 2 - n$) shares were stacked, the probability of appearing black pixels on the stacked shares increased to k/n; while for the white pixels, the probability of appearing as black pixels remained as $1/n$. After stacking all shares, black regions of the secret image could be completely reconstructed and were recognized by the human eye owing to the large contrast between black and white pixels.

Substantial work has been done on transformed domain VC based schemes also [6, 7]. A DWT-SVD (Discrete Wavelet Transform- Singular Value Decomposition) approach was suggested by Wang and Chen [6] where first DWT is applied to the host image followed by SVD. A feature vector is subsequently created and k-means clustering is used to classify into two clusters. A master share is generated in the next stage and ownership share constructed using the master share and secret image. In a method devised by Rawat et al [7], Fractional Fourier transform (FrFT) is used as a major tool followed by SVD. The transform orders of FrFT act as the key for the algorithm providing it enhanced security. The problem with these techniques was that the shares were pseudo random noise like-patterns carrying no visual information and hence raised the suspicion of cryptanalysts. To combat this drawback work was done to generate meaningful binary images as shares. This reduced suspicion and made detection even more improbable, thus raising the security level.

III. Visual Cryptography Based Video Watermarking Schemes

A video is nothing but a sequence of images yet image watermarking techniques cannot be directly applied to videos owing to their three dimensional characteristics. In addition to their special preprocessing techniques, the temporal nature of videos has to be taken into account [1]. Redundancy between frames and a large volume of data makes it all the more difficult to perform watermarking in videos. Some common forms of attack on videos are frame swapping, frame averaging, frame dropping, statistical analysis, interpolation etc. which are unknown to the domain of image watermarking. Inter- video collusion attacks and intra-video collusion attacks are also issues which need to be addressed. Real time implementations of video watermarking techniques are generally much more complex than that of image watermarking which becomes an important issue.

Video watermarking schemes are used for various video applications such as copyright protection, copy control, fingerprinting, broadcast monitoring, video authentication, enhanced video coding etc. Some

traditional video watermarking schemes attempt to embed an entire watermark image within each video frame or within random video frames to give the appearance of a hidden watermark to the casual observer.
Neither embedding the same watermark to each frame nor embedding different watermarks in every frame of the video would be robust against all types of common attacks. Embedding identical watermark to each frame of the video leads to the problem of maintaining statistical perceptual invisibility. The collusion can estimate the watermark from each watermarked frame and obtain a refined estimate of the watermark by linear combination. The non-watermarked frame can be obtained with subtraction with the watermarked one. On the other hand, applying independent watermarks to each frame also presents a problem if regions in each frame have little or no motion between the consecutive frames. The motionless regions may be averaged to remove the independent watermarks. Previous schemes of video watermarking are based on the uncompressed domain but most of the videos on the internet are available in a compressed format. A few techniques have been developed in the recent years which perform video watermarking in the compressed domain [8-10]. A scheme proposed in [8] uses the phase angle of the motion vectors of macroblocks in the inter-frame to embed data in a video. A different approach has been suggested in [9] to achieve a lesser distortion to prediction error and lower data size overhead in comparison to [8]. Here, motion vectors whose associated macroblocks' prediction error is high are taken to be candidate motion vectors (CMV). The CMV's are then used to hide a bit of data in their horizontal and vertical components. Shanableh [10] later proposed two novel approaches to which gave a higher message extraction accuracy and payload. In the first approach message bits are concealed by modifying the quantization scale of the MPEG video. Feature extraction is performed by for individual macroblocks and a second order regression model is computed to predict the content of the hidden message. Though this procedure has a high level of prediction accuracy the payload is restricted to one bit per macroblock. The second approach proposed in [10] benefits from a high message payload with negligible drop in the PSNR levels. This solution uses Flexible Macroblock Ordering (FMO) to direct the encoder to create slice groups (independently coded and decoded units). Each slice group contains slices and macroblocks are assigned in any order to these slices. The slice group ID's of individual macroblocks may then be used for to indicate the message bits that are hidden in the slice groups. Since this method is compatible with H.264/AVC standards and is independent of the frame type being used (Intra frame Predicted frame or Bidirectional Frame) it is advantageous from the point of view of implementation. However, the drawback with this solution is that it increases the bitrate of the coded video. All of these schemes [8-10] modify the content of the host video which in turn affects the host video quality. Instead of mentioned traditional watermarking schemes, we can use VC based techniques effectively for copyright protection. In this section, we present some of the existing VC based watermarking schemes for videos.

A. VC based Video Watermarking in Spatial Domain

One of the earliest video watermarking approaches was proposed in 2006 by Houmansadr and Ghaemmaghami [11] in the spatial domain using VC which proved to be robust to collusion attacks and geometrical attacks. The proposed scheme is based on Naor and Shamir's (2, 2) visual secret sharing scheme and can be broadly categorized into Embedding of Watermark and Detection of Watermark stages.
Within the embedding stage, the algorithm begins with the share creation phase wherein the binary watermark image is split into two noise-like pseudo random shares. The binary format (0, 1) of the watermark information is converted to the (-1, +1) signed format which gives a pseudo-random watermark sequence which is approximately zero mean. In the following phase of the proposed algorithm, the frames of the video are temporally scrambled by the use of a Linear Feedback Shift Register (LFSR) as illustrated in Fig. 2(a). Initial condition of the LFSR serves as the private key in the watermark detection stage.

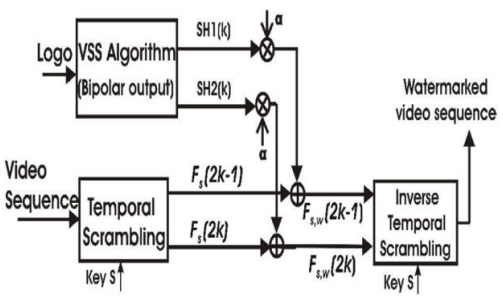

Figure 2(a). Block diagram for inserting watermark in [11]

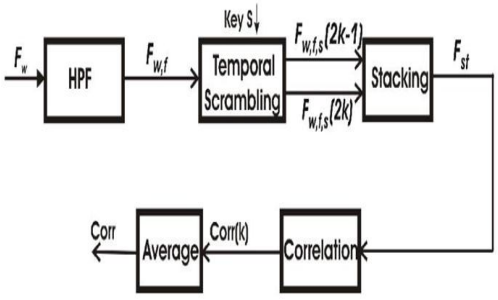

Figure 2(b). Block diagram for detecting watermark in [11]

A one to one mapping is maintained between the frames of the original video and the temporally scrambled video. The next phase which is the share insertion phase scales the shares by a parameter *'α'* (a parameter to determine the strength of the watermark which is fixed to be '3') and combines them with the scrambled video frames. The final watermarked video sequence is produced by the inverse temporal scrambling process. The watermark detection stage, shown in Fig. 2(b), begins with passing the watermarked video through a high pass filter (HPF) which preserves the high frequency components in the noise- like watermark sequence. Subsequently, the video is temporally scrambled once again such that the frames containing the shares now lie adjacent to each other. As a result L/2 stacked frames are obtained where a pixel by pixel comparison between the stacked frames are done, followed by a reduction of the stacked image from *(2M) X (2N)* pixels to *(M X N)* pixels. The detection algorithm uses the principle that stacking frames, containing corresponding shares of the logo, makes higher correlation with the logo, as compared to stacked frames containing non- relevant shares of the logo. The *Corr (k)* function gives a measure of the correlation between the L/2 stacked frames and the binary watermark, based on which we draw the conclusion about the presence or absence of the specified watermark.

$$Corr(k) = \frac{F_{st}(k) \bullet W}{\sqrt{E(F_{st}(k)) * E(W)}}, \; k = 1,...,[\frac{L}{2}] \qquad (1)$$

where W is the watermark, F_{st} is the stacked frame, $E(F_{st})$ returns the energy of the stacked frame, $E(W)$ gives the energy of the watermark and the dot returns the dot product.

In this simple and effective spatial domain method, the inserted watermark shows high resilience against some attacks, such as geometrical distortions and collusion attacks. However, the scheme is in spatial domain which provides a lower robustness to steganalysis in comparison to VC based watermarking techniques of the transformed domain. Further, since the shares are embedded into the host video in the watermark embedding stage, it alters the contents of the host and hence degrades it.

B. VC based generation of Embedded Crypto-Watermarks

Later in 2008, Zeng and Pei [12] suggested a novel video diagnosing method where the generation of crypto-watermarks was carried out by using the concept of visual cryptography. Here, significant information in the form of crypto-watermarks is embedded into the video through a Dual Domain Quaternary Watermarking Algorithm which lends robustness to the scheme. The proposed method can identify the attack category (frame attack and temporal attack) and the video authentication type (whether video is a watermarked video or non-watermarked video) by means of the BER (bit error rate).

The first stage of the algorithm is the generation of such crypto- watermarks while the next stage embeds the crypto-watermarks using the quaternary watermarking algorithm. The crypto-watermarks are generated through visual cryptography from binary images and have different resistances against different attacks. Four crypto-watermarks, namely first watermark ($\mathbf{W_1}$), second watermark ($\mathbf{W_2}$), intra-watermark ($\mathbf{W_3}$) and inter-watermark ($\mathbf{W_4}$) are generated as shown in Fig.3. $\mathbf{W_1}$ and $\mathbf{W_2}$ form the quaternary watermark ($\mathbf{W_q}$). This quaternary watermark is added into the intra frame in the DCT domain in the embedding stage. During the watermark extraction stage at the receiver end, the data stream is divided into 8x8 non overlapping blocks and then $\mathbf{W^*_q}$ is extracted by calculating sample values in the DCT domain.

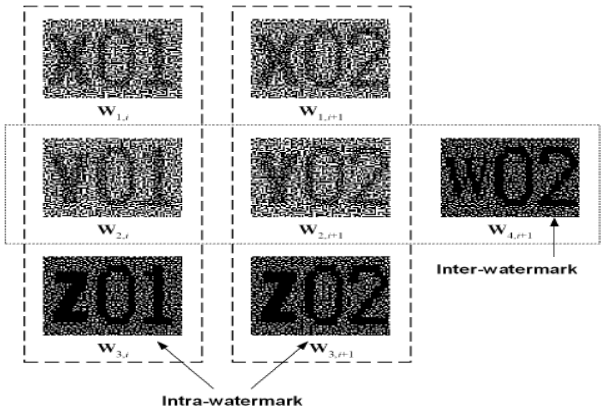

Figure 3. Generation of crypto-watermarks in [12]

The bit-error-rate (BER) between the extracted watermarks of the suspected video and the original crypto-watermarks is measured. Analysis of BER determines the nature of attack on the video. Based on a comparison of BER's between the first, second, intra and inter watermarks, status of frame attack is assigned. The status can be used to diagnose a video to be a non-watermarked video, authorized video, recompressed video and unauthorized frame inserted video.

Important applications of this methodology include dispute resolving, content identity verification and prevention of illegal video editing. However, the decryption process is not done by merely overlaying the shares. Since the watermark extraction process involves computations in the DCT domain followed by calculation of sample, it causes a computational overhead. Thus the inherent advantage of visual cryptography that is, extracting the secret information directly by the human visual system without the use of any complex computational process, is compromised. Also, similar to the method proposed in [11], this is an intrusive method and operates by directly embedding the watermark into the contents of the host.

C. VC based Video Watermarking using scene averaged image

In both previous mentioned techniques, content of host audio is modified. In 2010, Vashistha et al. proposed a method [13] that employs (2, 2) visual cryptography, scene change detection and extraction of features from scene to create *Verification Information* (VI). The authors' have rightly coined the term '*non-intrusive watermarking*' for visual cryptographic schemes since the information of the watermark has been extracted by creation of shares applying the principles of visual cryptography rather than embedding watermark information directly into the cover content (host image or video). This is indeed a major advantage over the previously mentioned schemes of [11] and [12]. The process to generate *VI* for watermark pattern *W* of size ($h \times l$) and an original 256 gray-leveled image *I* of size ($m \times n$) with the help of a secret key, *S* (a random number) and by the rule shown in Fig. 4(a) and 4(b). The *VI* is constructed by assembling all the *(Vi1, Vi2)* pairs. In the verification process, the authenticity of the image *I'* is assessed by using the inverse process. The above process is used in the context of videos by first performing scene change detection and then by forming a scene averaged image which is converted into grey scale for computing the *Verification Information (VI).* The number of scenes detected decides the number of *VI* vectors since these two values have to be necessarily equal. The *VI* vector is thus one of the shares generated from the watermark pattern and the secret image.

Since no data is embedded into the host video in this technique, the method is resilient to attacks aimed at distorting the data embedded into videos. The method is particularly effective against frame averaging, frame dropping, frame swapping and interpolation attacks. All watermarked scenes, and not just individual frames, need to be dropped for an effective attack. Dropping of scenes makes illegal copying and distribution pointless and thus automatically discourages malpractices. The scheme can survive as much as a 50% frame drop attack. However, when the *VI* of a different scene is used, the extracted watermark quality is highly degraded. Also, the scheme is in the spatial domain which makes it less robust than its transform domain counterparts.

Pixel in watermark pattern	Share 1	Share 2	Share 1 & 2 superimposed
■	(1,0)	(0,1)	(1,1)
■	(0,1)	(1,0)	(1,1)
□	(1,0)	(1,0)	(1,0)
□	(0,1)	(0,1)	(0,1)

Figure 4 (a). Visual Threshold Scheme of [13]

Color of i^{th} pixel in W	The MSB of R_i^{th} pixel of image I	Assign (V_{i1}, V_{i2}) of VI to be
Black	1	(0,1)
Black	0	(1,0)
White	1	(1,0)
White	0	(0,1)

Figure 4 (b). Rules to assign values for *VI* in [13]

D. VC based Video Watermarking using scene change detection

In 2011, Singh et al. [14] implemented VC based scheme based on DWT transform domain and scene change detection. Here, 1- level Discrete Wavelet Transform (DWT) is applied on averaged frame and features are

extracted from LL subband. The watermark is split into sub-watermarks, the number of sub-watermarks being equal to the number of detected scenes. Frame mean (I) of all frames in a scene and global mean (μ) of

the frame mean in a scene are found by taking the average of all corresponding pixel values in all frames in the same scene and the average of all pixel values in the frame mean (I) in the same scene respectively. Next, the construction of owner's share is done by checking the pixel value of the binary watermark and comparing the pixel value of the frame mean of same scene of the video with the global mean. Since, different parts of a single watermark are used in different scenes while the same sub-watermark is used for the different frames of a same scene the algorithm becomes robust to frame attacks like frame averaging, frame dropping, frame swapping and interpolation attacks. The identification share is generated by comparing the frame mean (I') of the suspected video with the global mean (μ') of this frame mean. The stacking of both the shares reveals copyright information. An overview of this scheme is demonstrated in Fig. 5(a) and 5(b). The robustness of DWT to noise attacks and the security and simplicity of VC makes this technique easy to implement.

E. VC based Video Watermarking using unique frame identification

In [13] and [14], authors have used all the frames belonging to one scene in order to extract features and create share. Kumar and Hensman [15] proposed a scheme which pre-process video in order to extract unique frames from a given video before watermarking. Hence instead of embedding watermark in all frames, the watermark is distributed only in selected unique frames. Here, DWT based similarity approach, first, segregates the video into similar and dissimilar frames. Following this, *k* shares are created where *k* is the number of unique frames which were detected in the previous stage through DWT. The watermark image is divided into *n* size sub blocks, and then each *n* block is divided into *k* sub blocks. The *i* th block from this *k* block sequence will be taken to build the *i* th sub image. In the same way, all sub images will be composed to generate the cryptography watermark. Hence, selected frames only will contain a fractional number of pixels from the watermark logo until the entire logo is distributed over different frames. This gives the advantage that information from a single frame will not reveal the watermark information or even give any indication that it contains a fraction of the watermark pixels. Further, he used a lossless/reversible data hiding technique to embed the watermark. The stage by stage representation of the multi layered structure for this scheme is illustrated in Fig.6. Here, the author claims that the video frame before and after watermarking may appear to be the same.

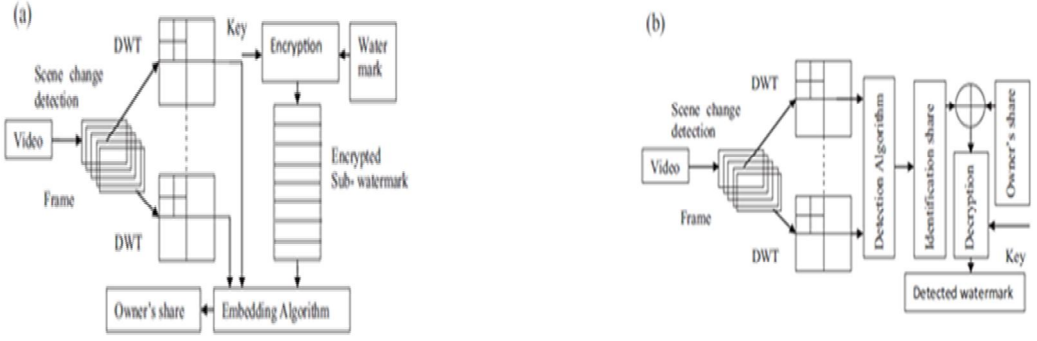

Figure 5 .Overview of the watermarking process in [14] (a) generation of owner's share and (b) generation of identification share.

IV. Performance Comparison Of The Reviewed Schemes

Though all above mentioned VC based video watermarking schemes have tried to achieve high imperceptibility, high robustness, they suffer from limitations imposed by VC technique itself. For any VC scheme, resolution of extracted secret watermark binary image is degraded due to pixel expansion [2]. Here, pixel expansion increases apparent randomness and security but often leads to a poorer quality of extracted watermark. Therefore, a compromise between security and resolution should be made for successful implementation of these VC based schemes. Also, certain VC schemes operate by dividing the host image or video into non-overlapping blocks and then by selecting only a few blocks on which the feature extraction techniques are applied [7, 14]. When a smaller block size is chosen, the number of blocks obviously

increases. Thus, there is more randomness in selecting the blocks which enhances the security of the scheme. On the other hand, a larger block size captures the features of the host more effectively as compared to a smaller block size. Therefore, a tradeoff needs to be achieved in between level of security and feature extraction accuracy too.

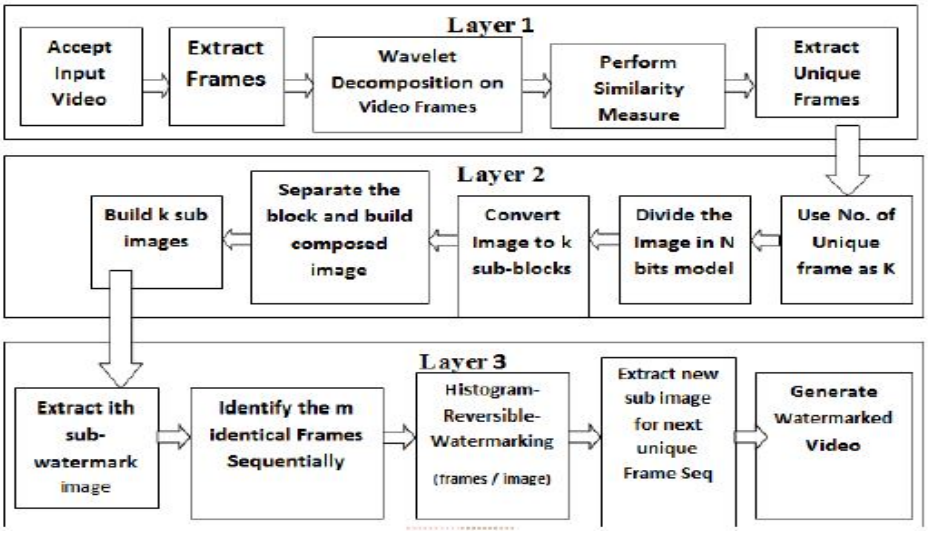

Figure 6. Layered design of the approach proposed in [15]

TABLE I. Performance Comparison of Various VC Schemes for Videos

S. No.	Proposed Scheme	Year	No. Of Shares	Domain	Intrusive/ Non-intrusive	Techniques Used	Performance mentioned in related work
1	Houmansadr and Ghaemmagh-ami [11]	2006	2	Spatial	intrusive	Temporal Scrambling, Stacking, Correlation	For 50 % frame cropping decrement in correlation coefficient 16%; For 8 times frame scaling, decrement in correlation coefficient 39%;
2	Zeng and Pei [12]	2008	4	Dual Domain (DCT and Spatial)	intrusive	Inter-Frame and Intra-Frame crypto watermark generation	Average PSNR found to be 52.78 dB for original frames and 42.18 dB for watermark; capable of identifying different types of attacks.
3	Vashistha et al. [13]	2010	2	Spatial	non-intrusive	Construction of Verification Information vector, Scene change detection by segmentation based on colour difference histogram, scene averaging.	Survives as much as a 50% frame drop
4	Singh et al. [14]	2013	2	DWT	non-intrusive	Scene change detection, scene averaging	NC above 0.95 for all kinds of frame attacks
5	Kumar and Hensman [15]	2013	*k*	DWT	intrusive	DWT for unique frame extraction, Multi-Layer Approach	Not mentioned

A watermarking scheme is evaluated on the basis of criteria like perceptibility, reliability, robustness, capacity, speed of implementation and statistical detectability. MSE (Mean Square Error), PSNR (Peak-Signal–to-Noise Ratio) and NC (Normalized Correlation) are some of the metrics which are used for comparison. MSE is defined as the mean square error between the pixels of the original image $\boldsymbol{H}$ and the attacked image $\hat{H}$

$$MSE = \frac{1}{MN}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}[H(i,j)-\hat{H}(i,j)]^2 \qquad (2)$$

PSNR gives us a measure of the degree of distortion to the watermark.

$$PSNR = 10 \log_{10} \left(\frac{255^2}{MSE} \right) \text{dB} \quad (3)$$

NC is the measure of similarity between the original and extracted watermarks.

$$NC = \frac{\sum_{i=1}^{m} \sum_{j=1}^{n} \overline{S_{i,j} \oplus S''_{i,j}}}{m \times n} \quad (4)$$

where $m \times n$ is the image size, $S_{i,j}$ and $S''_{i,j}$ represent original and extracted watermarks respectively. In mentioned schemes, the watermarked videos were subjected to variety of attacks like frame attacks (like frame swapping, frame averaging, frame dropping, statistical analysis, interpolation etc.), noise attacks (like impulse and Gaussian noise etc.) and geometrical attacks (like cropping, reshaping, resizing, rotating etc.). Apart from these, blurring, filtering, sharpening, scaling and JPEG compression attacks were also used to ascertain the robustness. Here, we have provided comparison of the above mentioned techniques in Table I.

V. CONCLUSION

Visual Cryptography has proven to be a simple, robust and non-intrusive watermarking technique. Though VC is widely used in case of image watermarking, video watermarking imposes more challenges. The feature extraction techniques applied for creating shares from videos are more complex than images. Generally Group of Pictures (GOPs), scene change detection, unique frame identifications etc. are considered in these feature extraction techniques. Video files have a larger size compared to simple images; this provides an excellent opportunity to add more secret information. Utilizing the power of visual secret sharing methods for videos in transform domain may offer a very attractive and robust solution for different sectors like defence or military video based communication services, music industries to establish their rightful copyright ownerships, digital video forensic applications etc.

REFERENCES

[1] Hartung F, Kutter M. "Multimedia watermarking techniques." Proc IEEE 1999; 87(7 (July)).

[2] Naor M. and Shamir A., "Visual Cryptography," in Proceedings of Advances in Cryptology-EUROCRYPT, Lecture Notes in Computer Science, Berlin, pp. 1-12, 1995.

[3] G. Ateniese, C. Blundo, A. De Santis and D. R. Stinson, "Visual cryptography for general access structures", Information and Computation 129 (1996), 86-106.

[4] W. P. Fang and J. C. Lin, "Progressive viewing and sharing of sensitive images," Patt. Recog. Image Anal., vol. 16, no. 4, pp. 638–642, 2006.

[5] Young-Chang Hou and Zen-Yu Quan, "Progressive Visual Cryptography with Unexpanded Shares", IEEE Transactions On Circuits And Systems For Video Technology, Vol. 21, No. 11, November 2011, pp. 1760-1764.

[6] M.S.Wang, W.C.Chen,"A Hybrid DWT-SVD Copyright Protection Scheme Based On K-Means Clustering And Visual Cryptography", Computer Standards &Interfaces, 31 (2009)757–762.

[7] Rawat, S and Balasubramanian Raman, "A Blind Watermarking Algorithm Based On Fractional Fourier Transform And Visual Cryptography," Elsevier Signal Processing, Vol 92 ,2012, pp. 1480–1491

[8] Ding-Yu Fang, Long-Wen Chang, "Data Hiding For Digital Video with Phase of Motion Vector," IEEE International Symposium on Circuits and Systems, 2006, pp. 1422- 1425.

[9] Aly, H., "Data Hiding In Motion Vectors Of Compressed Video Based On Their Associated Prediction Error," IEEE Transactions on Information and Forensics Security, Vol. 6, No. 21, Mar 2011, pp. 14–18.

[10] Shanableh, T., "Data Hiding in MPEG Video Files Using Multivariate Regression and Flexible Macroblock Ordering," IEEE Transactions on Information Forensics and Security, Vol. 7, No. 2, Apr 2012, pp. 455–464.

[11] Amir Houmansadr and Shahrokh Ghaemmaghami, "A Novel Video Watermarking Method Using Visual Cryptography," IEEE International Conference on Engineering of Intelligent Systems, Islamabad, Pakistan, 2006.

[12] Yi-Chong Zeng, Soo-Chang Pei, " Automatic Video Diagnosing Method Using Embedded Crypto-Watermarks", IEEE International Symposium on Circuits and Systems, 2008. (ISCAS 2008).dg

[13] Aditya Vashistha, Rajarathnam Nallusamy, Amitabha Das, Sanjoy Paul," Watermarking Video Content Using Visual Cryptography And Scene Averaged Image", IEEE Conference, 2010.

[14] Rupachandra Singh, Th., Manglem Kh Singh, , and Sudipta Roy "Video Watermarking Scheme Based On Visual Cryptography And Scene Change Detection," Elsevier International Journal of Electronics and Communications (AEU) , Vol 67, Jan 2013, pp. 645- 651.

[15] Kumar, M. and Hensman, A. "Robust Digital Video Watermarking Using Reversible Data Hiding and Visual Cryptography", ISSC conference 2013 at LYIT, Ireland.